**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 285**

Security Equipment

**Security hardware**

1. What is meant by data integrity?

Data integrity is the assurance that data is accurate and reliable, and available in a timely manner.

1. Biometrics
   1. Describe biometric security.

Biometric security is the use of human characteristics as a means of protection. For example, retina scanning software or fingerprint recognition can provide a unique password to a system.

* 1. Why does it appeal to security managers?

It appeals to security managers because it is nearly impossible to steal someone’s biometric characteristics.

* 1. List the common biometric devices.

The biometric devices include voice recognition, fingerprint recognition, hand geometry, signature verification, facial recognition and iris recognition.

* 1. What are the concerns of biometric technology?

The concerns of biometric security are that most devices are invasive to the user and require a lot of money to buy and maintain.

1. Swipe cards
   1. Describe the nature of a swipe card.

Swipe cards are a plastic card with a magnetic strip on one side and user details stamped onto the other. For example in a credit card, the magnetic strip contains data about the owner of the card including their PIN. They are used for electronic transfer or in swipe card locks for doors.

* 1. What is a limitation of the swipe card?

The limitations of a swipe card are that it can be easily damaged by magnetic fields, and offer little protection from theft.

1. Smart cards

Smart cards have a microchip embedded in them to store and manipulate data. They may contain secure information about medical history, emergency care data, etc. and can carry as much as 10MB of data.

1. Security tokens

Security token are small electronic devices that provide a constantly changing authentication code. A username and password is input into the device, and provides the password required to access secure sites such as online banking.

1. Mobile phone secure code
   1. How does this level of authentication work?

Mobile phone secure cards authenticate by sending a authentication password to the users mobile phone which they then enter before the transaction is processed.

**Power protection**

Outline the characteristics of the following:

1. Surge protector

Surge protectors protect electrical equipment against overvoltage caused by a power surge, and will instead take damage in place of the equipment it is protecting.

1. Uninterruptible power supply, (UPS)

UPS provide a high quality surge protector and battery power in case of a power failure. They can then maintain protecting data for the life of the battery, about 30 minutes, which is enough to save important files and shut down the equipment.

**Strategies for avoiding system failure, p 288**

1. What is meant by redundancy?

Redundancy is a means of data security which provides backup to systems in the case that one of the devices fail. The other devices then share the load of the failed device and continue to run normally until the device is replaced.

1. What is meant be a fault-tolerant server?

A fault tolerant server is one that has no single part critical to its operation, and uses redundancy to protect the devices.

1. Redundancy through multiple hard drives or fault-tolerant equipment
   1. Describe how this redundancy works.

If one part fails, the other hard drives or mirrored machines can take over its job and keep the system running until the part is replaced.

* 1. What is meant by RAID technology

RAID technology (redundant array of inexpensive disks) is used on a computer network to spread the data over several hard drives. If one fails, the others can piece together the missing data and rebuild the system. Damaged disks must be replaced quickly because if more than one fails, the data would become too hard to recover.

1. Redundancy through mirrored servers or machines
   1. Why is the RAID solution preferable to this solution?

Mirrored servers or machines are back up machines which contain duplicates of the data stored on the normal machine. RAID is preferable to this because the disks are inexpensive and replacing failed parts is less expensive.

**Backup Media**

1. There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?

When deciding which backup media to use, consider the software you will use, the cost of the drive or writer, and the speed and compatibility.

Three categories of backup media:

List the characteristics of the following backup media:

**Magnetic media**

1. hard disk drive

A second internal hard drive can be used to backup data. It is best to have an external or removable hard drive that can easily be taken in the event of an emergency. The users may also backup data to networked hard drives located offsite which are capable of holding data from multiple machines.

1. Magnetic tapes

Magnetic tapes are a cheap means of backing up files, but slow to save and restore files with. They must be read and accessed sequentially, and have larger storage capacity than CDs or DVDs.

**Optical media**

1. Compact disc

Compact discs are removable storage media that can hold up to 700MB of data and either come as rewritable or read only.

1. DVD

DVDs have a larger capacity of 17GB and either come as rewritable or read only. (double sided)

1. Blu-ray

Blu-ray have a larger capacity again of 50 GB and use a blue laser to read the dual layered disc, also allowing high definition films to be stored.

**Solid-state drives**

1. USB storage devices

Solid state drives such as USB are convenient brcause of their small size, and have less chance to breakdown. However they usually only have small storage space – between 2 and 16GB.

**Online backups**

1. Why do organisations use this form of backup?

Organisations backup online so that the data can be accessed at multiple sites without having to physically transfer the data. In the event of an emergency at a particular site, all the data can still be accessed at another with access to the online server.

1. Describe an enterprise storage system.

Enterprise storage systems involve using multiple techniques for storing data so that it is secure, for example RAID technology where multiple disks or drives are used to back up data on to. If one disk were to break, the others have sufficient information to recover whatever data was lost, until the disk can be replaced. They also include internet backups and other networked storage devices.

**Surveillance technology, p 292**

Describe the nature of the following items of surveillance equipment used in offices:

1. Packet sniffers

Packet sniffers are used for internet and email and their purpose is to monitor the content carried in emails and other data on the network.

1. Desktop monitoring programs

These programs log all the programs that are opened on the desktop, and are mostly used by hackers.

1. Log files

Log files are a record of the URL history of the sites accessed on the web browser, networks, etc.

1. Closed-circuit television, (CCTV)

Closed circuit television is a visual recording of a particular area, where security cameras are used to view the activities of customers and employees. These are usually backed up onto tapes and stored for a short period in time in case the need to be recalled for evidence of a crime, etc.

1. Telephones

Employers can tap the phones of their employees to ensure they are only doing what they are authorised to do so. In most cases, they only wish to restrict conversations to company related business, or to ensure that a high quality service is provided to customers on the phone.

1. Audit trails

Audit trails allow employers to trace transactions or other forms of activity in the system. It can contain log files to check up on what sites are being accessed, programs used, etc. This system can b automated so the supervisors only need intervene when the system finds an irregularity.

**Physical security devices:** List the options for physically securing your data

Lockable disk boxes, safes and special access restricted rooms, and security cables being attached to items are all physical means of security, as well as embedding microchips into products such as in super markets to set off alarms in the case of shop theft.